REMARKS

In view of the above amendments and the following remarks, reconsideration of the rejections and further examination are respectfully requested.

Claims 11-16, 19, and 23 remain cancelled and claims 18 and 20 have been newly cancelled.

Further, independent claims 1, 17, 21, 22, and 24 have been amended to clarify the features of the claimed invention and to further distinguish the claimed invention from the prior art referenced in the rejections discussed below. It is noted that the amendments of the claims are supported, at least, by page 80, lines 5-16, and page 83, line 21 to page 85, line 2 of the specification. In addition, dependent claims 3-10 have been amended to remain consistant with amended independent claim 1.

Claims 1 and 2 were rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Specifically, claim 1 was rejected for reciting an apparatus claim without any structural component and consisting solely of language that is implemented with only software and for not providing any functional interrelationship to any software from hardware structural components to provide certain function that is processed by a computer.

In this regard, Applicants respectfully submit that amended claim 1 recites a plurality of structural limitations. For example, amended claim 1 recites a receiving unit configured to receive, from the terminal apparatus, a supply request and a key supply unit configured to supply to the terminal apparatus the decryption key. Applicants submit that at least these components are structural limitations. Thus, withdrawal of this rejection is respectfully requested.

Claims 1, 2, 21, 22 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Maeda (U.S. 2004/0228487) in view of Alve et al. (U.S. 2004/0076955). Further, claims 3, 4-9, 10 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Maeda in view of various combinations of Alve et al., Marshall et al. (U.S. 4,866,707), Mooney et al. (U.S. 6,351,813), and Ito et al. (U.S. 7,137,025). These rejections are believed clearly inapplicable to amended independent claims 1, 17, 21, 22, and 24 and the claims that depend therefrom for the following reasons.

Amended independent claim 1 recites a supply determining unit configured to determine whether the terminal manages content-usage (i.e., a first-type terminal), and whether the terminal does not manage content-usage (i.e., a second-type terminal). Further, claim 1 recites a key supply unit configured to, supply to the terminal, (i) the decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is determined to be of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is determined to be of the second-type. In addition, claim 1 recites that the supply request includes one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, and the second information indicating that the encrypted content is stored on a portable recording medium inserted into the terminal apparatus. Moreover, claim 1 recites that the supply determining unit determines, based on the received supply request, whether the terminal apparatus records the encrypted content on the portable recording medium, and determines that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable

recording medium. The Maeda, Alve, Marshall, Mooney and Ito references, or any combination thereof, fail to disclose or suggest the above-mentioned distinguishing features.

The above mentioned 35 U.S.C. § 103(a) rejection of claims 1, 2 and 17-24 relies on Maeda for teaching the supplying of the decryption key and the key-usage period by the key supply unit, as recited in claim 1.

However, Maeda teaches that, if use of content S7 is judged to be permitted, then the usage rights judgment unit 15 continuously transmits a usage permission signal S8 for an entire duration of which the content S7 can be used. Further, Maeda teaches that, if use of content S7 is judged to not be permitted, then the usage rights judgment unit 15 stops transmitting a usage permission signal S8 to prohibit the use of the content S7 (see paragraph [0058] and [0059], lines 6-8). In addition, as a result of the above-described operation (as described in paragraph [0059]), continuous use of content S7 requires a continuous and ongoing transmission of the usage permission signal S8 between the usage rights judgment unit 15 and the decryption unit 14.

Thus, in view of the above, it is clear that Maeda teaches that an ongoing and continuous transmission of the usage permission signal is required during the use of the content in order to continue using content, but fails to disclose or suggest the key supply unit configured to, supply to the terminal, (i) a decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is of the second-type, as required by claim 1.

In other words, Maeda fails to disclose or suggest supplying a decryption key and supplying a key-usage period related to the decryption key (i.e., one transmission of two items of

data from the key supply unit) in order for content to be used, as required by claim 1, because Maeda requires a continuous transmission of a permission signal in order for content to be used.

Please note that one of the benefits of the configuration recited in claim 1 is that based on the type of terminal requesting/receiving content, the key supply unit supplies a decryption key and a key-usage period (transmission is not required to be continuous for the entire duration of content usage), which provides an efficient way of allowing and/or restricting use of content. In light of the discussion above, the Maeda reference does not provide the above-mentioned result of the structure required by claim 1 because a continuous transmission of a usage permission signal for allowing use of content is a different and less efficient structure for allowing and/or restricting use of content.

Therefore, because of the above-mentioned distinctions it is believed clear that the features of the key supply unit, as recited in claim 1, would not have been obvious or result from the disclosure of Maeda.

In this regard, the Examiner submits by reciting paragraphs [0042] and [0049] in the Official Action dated on August 01, 2008 that Maeda discloses the key supply unit configured to, supply to the terminal, (i) a decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is of the second-type, wherein the supply determining unit determines that the terminal apparatus is of the first-type when the supply determining unit determines that the terminal apparatus records the encrypted content on the portable recording medium, as required by claim 1.

However, paragraph [0042] merely explains a structure of a physical layer of the user area 1008 within the SD memory card, and paragraph [0049] merely teaches directories and files in the protected area 1003 of the SD memory card. Rather, as above discussed, Maeda teaches that, if use of content S7 is judged to be permitted, then the usage rights judgment unit 15 transmits a usage permission signal S8 to decryption unit 14 for the duration of remaining usage period S5, while, if use of content S7 is judged to not be permitted, then the usage rights judgment unit 15 stops transmitting a usage permission signal S8 to prohibit the use of the content S7 (see paragraph [0058]). Thus, these recited portions do not contain any disclosures regarding al least a key supply unit configured to, supply to the terminal, (i) a decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is of the second-type.

Therefore, Applicants submit that Maeda fails to disclose at least a key supply unit configured to, supply to the terminal, (i) a decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is of the second-type, as recited in, for example, claim 1.

Further, the Examiner admits that Maeda fails to disclose a supply determining unit configured to determine whether the terminal apparatus is a terminal apparatus of a first-type that manages a content-usage period, and configured to determine whether the terminal apparatus is a

terminal apparatus of a second-type that does not manage the content-usage period, and determine that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium.

In setting forth the rejection, the Examiner relies on Alve regarding that which the Examiner admits is lacking in the Maeda. Alve relates to a system in which content providers identify their content as protected by watermarking the content. Consumers use compliant devices to access protected content. All of a user's compliant devices can be organized into an authorized domain. The authorized domain is used by content providers to create a logical boundary in which they can allow users increased freedom to use their content.

Alve also teaches that when an authorized border device receives content from a content provider (Fig.2a block 200), the authorized border device checks whether the content is watermarked (Fig.2a block 210). The authorized border device creates a content key and encrypts the received content with it when the content is watermarked (Fig.2a block 220). The authorized border device checks whether a transfer of the received content out of the authorized domain is allowed (Fig.2a block 230). The authorized border device encrypts the content key with a domain key when the transfer of the received content out of the authorized domain is not allowed (Fig.2a block 235). The authorized border device checks whether usage state is unrestricted when the transfer of the received content out of the authorized domain is allowed (Fig.2b block 240). The authorized border device encrypts the content key with a device public key of the authorized border device when the usage state is restricted in some way (Fig.2b block 245, and paragraphs [0039]-[0057]). In other words, Alve teaches that the authorized border

device encrypts the content key when the usage state is restricted, while the authorized border device does not encrypt the content key when the usage state is not restricted.

Alve further teaches that when an authorized device moves or copies the received content to another authorized device, the authorized device checks whether another authorized device is within the authorized domain (Fig.3a block 310). The authorized device checks whether usage state is unrestricted when another authorized device is within the authorized domain (Fig.3a block 320). The authorized device transfers the received content to another authorized device when the usage state is unrestricted (Fig.3b block 360). The authorized device checks whether the usage state indicates that a transfer of the received content is allowed (Fig.3a block 330). The authorized device decrypts the content key with a private key of the authorized device and encrypts the content key with a public key of another authorized device when the transfer of the received content is allowed (Fig.3b blocks 340 and 350). Then, the authorized device transfers the received content to another authorized device (Fig.3b block 360 and paragraphs [0058]-[0060]). In other words, Alve teaches that the authorized device transfers the received content to another authorized device without retargeting the content key when the usage state is unrestricted, while the authorized device retargets the content key and transfers the received content to another authorized device when the usage state is restricted.

However, Alve fails to disclose the following features recited in, for example, claim 1:

1) a key supply unit configured to, supply to the terminal, (i) a decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is of the first-type, and (ii) the

decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is of the second-type;

2) a supply determining unit configured to determine whether the terminal apparatus is a terminal apparatus of a first-type that manages a content-usage period, and whether the terminal apparatus is a terminal apparatus of a second-type that does not manage the content-usage period, and to determine that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium;

3) the supply request includes one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, the second information indicating that the encrypted content is stored onto a portable recording medium inserted into the terminal apparatus;

4) the supply determining unit determines whether the terminal apparatus records the encrypted content on the portable recording medium, based on the received supply request; and

5) the supply determining unit determines that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium.

Rather, as above explained, Alve merely teaches that the authorized border device encrypts the content key when the usage state is restricted, while the authorized border device does not encrypt the content key when the usage state is not restricted (Figs.2a and 2b, and paragraphs [0039]-[0057]). In other words, in Alve, the same content key is used when the

usage state is restricted and when the usage state is not restricted, regardless of whether the content key is encrypted or not. Alve also teaches that the authorized device transfers the received content to another authorized device without retargeting the content key when the usage state is unrestricted, while the authorized device retargets the content key and transfers the received content to another authorized device when the usage state is restricted (Figs.3a and 3b, and paragraphs [0058]-[0060]). In other words, in Alve, the same content key is used when the usage state is unrestricted and when the usage state is restricted, regardless of whether the content key is retargeted or not. Thus, Alve does not contain any disclosures regarding 1) a key supply unit configured to, supply to the terminal, (i) a decryption key and a key-usage period, which imposes a restriction on usage of content and is related to the decryption key, when the terminal is of the first-type, and (ii) the decryption key, without the key-usage period such that a restriction on usage of content is not imposed on the terminal, when the terminal is of the second-type.

Further, as above discussed, Alve merely teaches usage state information indicating whether the usage state is restricted (see. paragraph [0045]) and a voucher indicating when the usage state is restricted (see. paragraph [0060]). Thus, Alve does not contain any disclosures regarding at least 3) a supply request including one of first information and second information, the first information indicating that the encrypted content is stored in the terminal apparatus, the second information indicating that the encrypted content is stored onto a portable recording medium inserted into the terminal apparatus. For this reason, Alve fails to disclose 4) a supply determining unit that determines whether the terminal apparatus records the encrypted content on the portable recording medium, based on the received supply request, as well as 5) a supply

determining unit that determines that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium. For the deficiency of 4) and 5), Applicants submit that Alve also fails to disclose 3) a supply determining unit configured to determine whether the terminal apparatus is a terminal apparatus of a first-type that manages a content-usage period, and whether the terminal apparatus is a terminal apparatus of a second-type that does not manage the content-usage period, and to determine that the terminal apparatus is of the first-type when it is determined that the terminal apparatus records the encrypted content on the portable recording medium.

Therefore, because of the above-mentioned distinctions it is believed clear that the features recited in claim 1 would not have been obvious or result from any combination of Maeda and/or Alve.

Furthermore, there is no disclosure or suggestion in Maeda and Alve or elsewhere in the prior art of record which would have caused a person of ordinary skill in the art to modify Maeda and/or Alve to obtain the invention of independent claim 1. Accordingly, it is respectfully submitted that independent claim 1 and claims 2-10 which depend therefrom are clearly allowable over the prior art of record.

Regarding dependent claims 2-10, which were rejected under 35 U.S.C. § 103(a) as being unpatentable over Maeda in view of various combinations of the Alve, Marshall, and Mooney references (secondary references), it is respectfully submitted that these secondary references do not disclose or suggest the above-discussed distinguishing features of independent claim 1 which are lacking from the Maeda and Alve references. Therefore, no obvious combination of Maeda

with any of the secondary references would result in, or otherwise render obvious, the invention recited independent claim 1 and claims 2-10 which depend therefrom.

Amended independent claims 21, 22 and 24 recite a system, method, and program, respectively. Amended claims 21, 22 and 24 recite features that correspond to the above-mentioned distinguishing features of independent claim 1 (e.g., determination of the type of terminal apparatus, such as a first-type terminal apparatus and a second-type terminal apparatus, and supplying a decryption key or a decryption key and a key-usage period based on the type of terminal apparatus). Thus, for the same reasons discussed above, it is respectfully submitted that claims 21, 22 and 24 are allowable over Maeda, Alve, Marshall, and Mooney.

Regarding the 35 U.S.C. § 103(a) rejection of claim 17, it is noted that independent claim 17 now recites a portable recording medium including, in part, a key reception unit configured to (1) receive a decryption key and a key-usage period from a key delivery apparatus, a key storage unit configured to (2) store the decryption key and the key-usage period, a determining unit configured to (3) receive search information from the key delivery apparatus and (4) determine whether the decryption key is stored in the portable recording medium based on the search information, and a notifying unit configured to (5) transmit predetermined information indicating that the decryption key is stored in the portable recording medium. The predetermined information (6) indicates that the decryption key is stored on the portable recording medium and is transmitted when the proprietary determining unit determines that the decryption key is stored on the portable recording medium.

The Maeda, and Ito references, or any combination thereof, fail to disclose or suggest the above-mentioned distinguishing features (1)-(6) as recited in independent claim 17.

In setting forth the rejection, the Examiner admits that Maeda disclose at least a determining unit configured to (3) receive search information from the key delivery apparatus and (4) determine whether the decryption key is stored in the portable recording medium based on the search information, and a notifying unit configured to (5) transmit predetermined information indicating that the decryption key is stored in the portable recording medium, and the predetermined information (6) indicating that the decryption key is stored on the portable recording medium and that is transmitted when the proprietary determining unit determines that the decryption key is stored on the portable recording medium.

In the regards, the Examiner relies on Ito for teaching that which the Examiner admits is lacking in the Maeda. Ito relates to a system including an information transmitting apparatus, a key controlling apparatus, and an information receiving apparatus. Specifically, Ito teaches that the information transmitting apparatus transmits to the key controlling apparatus a date and time when secrecy protection is ended. Further, Ito teaches that the key controlling apparatus searches a key control table for an encryption key associated with the date and time, and the key controlling apparatus transmits the encryption key to the information transmitting apparatus. In addition, Ito teaches that the key controlling apparatus discloses to the information receiving apparatus a decryption key for the present date and time, in response to a request for the decryption key. Moreover, Ito teaches that the information transmitting apparatus, upon receipt of the encryption key, encrypts information using the encryption key and transmits to the information receiving apparatus the encrypted information. Finally, Ito teaches that the information receiving apparatus acquires the disclosed decryption key and encrypts the encrypted information using the decryption key.

However, Ito fails to disclose at least a notifying unit configured to (5) transmit predetermined information indicating that the decryption key is stored in the portable recording medium, and the predetermined information (6) indicating that the decryption key is stored on the portable recording medium and that is transmitted when the proprietary determining unit determines that the decryption key is stored on the portable recording medium, as required by claim 17.

Rather, Ito merely teaches a key controlling apparatus that receives form an information transmitting apparatus a date and time when secrecy protection is ended, searches for a key control table an encryption key associated with the received date and time, and transmits to the information transmitting apparatus the associated encryption key. In other words, in Ito, the key controlling apparatus merely transmits "an encryption key" to the information transmitting apparatus. Thus, Ito does not contain any disclosures regarding at least predetermined information indicating that the decryption key is stored on the portable recording medium and that is transmitted when the proprietary determining unit determines that the decryption key is stored on the portable recording medium, as recited in claim 17.

Further, Ito merely teaches an information transmitting apparatus that receives an encryption key from the key controlling apparatus, encrypts information using the received encryption key, and transmits the encrypted information to an information receiving apparatus.

In other words, in Ito, the information transmitting apparatus merely transmits "the encrypted information" to the information receiving apparatus. Thus, Ito does not contain any disclosures regarding at least predetermined information indicating that the decryption key is stored on the portable recording medium and that is transmitted when the proprietary

determining unit determines that the decryption key is stored on the portable recording medium, as required by claim 17.

Thus, it is clear that Ito fails to disclose or suggest at least predetermined information indicating that the decryption key is stored on the portable recording medium and that is transmitted when the proprietary determining unit determines that the decryption key is stored on the portable recording medium, as recited in claim 17. Therefore, because of the above-mentioned distinctions it is believed clear that the features of the key supply unit, as recited in claim 17, would not have been obvious or result from the disclosure of Maeda and Ito.

Furthermore, there is no disclosure or suggestion in Maeda or any of the secondary references which would have caused a person of ordinary skill in the art to modify Maeda and/or the secondary references to obtain the invention of independent claim 17. Accordingly, it is respectfully submitted that independent claim 17 is clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance and an early notification thereof is earnestly requested. The Examiner is invited to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,

Yuusaku OHTA et al.

/Andrew L. Dunlap/
2008.09.29 11:21:37 -04'00'

By:_____
Andrew L. Dunlap
Registration No. 60,554
Attorney for Applicants

ALD/led
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
September 29, 2008